Abstract

Method and arrangement for forming a secrete communication key for a predetermined asymmetric cryptographic key pair

After a key pair with a public key and a corresponding secrete key has been determined on the basis of an initial value, the initial value is made available to a user. The secrete key can be erased. When the user wishes to carry out a cryptographic operation based on the "Public-Key-Technology", the user enters the initial value into a computer and, upon utilization of the initial value, a secrete communication key is formed, which corresponds to the secrete key previously formed but erased since.

Sign. Figure 1